

JYVSECTEC's Approach to Cyber Exercises

Comprehensive Full-Scale Cyber Exercise

A realistic exercise aligned with organization-specific goals gives participants the opportunity to act in their actual organizational roles. The exercise model allows companies to examine their preparedness, management, and response processes and strengthens cooperation between organizations.

Benefits of a Full-Scale Cyber Exercise

- ▶ Provides a realistic and practical understanding of how cyberattacks can impact operations, how to respond to them, and how to recover from them in practice.
- ▶ Strengthens the ability to keep critical operations running, make decisions under realistic pressure, and coordinate activities with service providers and authorities.
- ▶ Develops the cyber resilience of individuals, teams, and the entire organization, while also creating opportunities to share lessons learned with colleagues in the same industry.





Ideal for High-Impact Cyber Exercises

JYVSECTEC's full-scale cyber exercise model is designed for comprehensive cyber security training and exercises. It enables exercises tailored to organizations and their cooperation partners or scaled to bring together entire business sectors, key stakeholders or operators of value chains. The model has been successfully used in Finland to enhance the resilience of critical infrastructure operators and strengthen collaboration between organizations and national cyber security authorities.

Scalable from Organization-Specific to National Cyber Exercises:

- ▶ Organization-Specific Cyber Exercises
- ▶ Sector-Level Cyber Exercises
- ▶ Multi-Sector and Cross-Sector Cyber Exercises
- ▶ National Cyber Exercises

Capabilities Developed Through the Exercise Model

JYVSECTEC's full-scale cyber exercise model strengthens both technical cyber security expertise and critical operational skills. It also helps participants improve problem-solving under pressure, conduct root-cause analysis, and deepen their understanding of risk management, business continuity, organizational resilience, and the wider business impact of cyber security incidents.

Technical Capabilities Developed

- ▶ Incident Response
- ▶ Digital Forensics
- ▶ Cyber Defense
- ▶ Situation Awareness
- ▶ Attack investigation

Operational Capabilities Developed

- ▶ Leadership
- ▶ Decision-making
- ▶ Crisis Management
- ▶ Crisis Communication
- ▶ Cross-organizational Collaboration

